Revised May 16, 2013

Annual Privacy Report of SDG&E

As Required by Decision (D.)11-07-056, Ordering Paragraph 3 And
D.12-08-045, Ordering Paragraph 3

Submitted to the CPUC

Introduction / Background

California Public Utilities Commission ("CPUC" or "Commission") Decision (D.)11-07-056 titled "Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company and San Diego Gas & Electric Company" or "Privacy Decision" was issued on July 29, 2011 and included a requirement in ordering paragraph (OP) 3 for an annual privacy report. Additionally, D.12-08-045 – "Decision Extending Privacy Protections to Customers of Gas Corporations and Community Choice Aggregators, and to Residential and Small Commercial Customers of Electric Service Providers" was issued on August 23, 2012 and also includes a requirement for a privacy report in OP 3.

Specifically, OP3 of D.11-07-056 states: *"Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company must each submit annual privacy reports to the Executive Director, commencing with calendar year 2012, no later than 120 days after the end of the calendar year. These annual reports must contain the information required to be reported annually by Rule 8(b) and Rule 9(c) of the Rules Regarding Privacy and Security Protections for Energy Usage Data in Attachment D of this decision."* D. 12-08-045 reiterates this requirement.

SDG&E's annual privacy report in response to D.11-07-056 and D.12-08-045 is included as Attachment 1.

Attachment D to the Privacy Decision is titled "Rules Regarding Privacy and Security Protections for Energy Usage Data" ("Attachment D Rules"). Sections 8(b) and 9(c) of the Attachment D Rules state:

> *"8(b) Notification of Breach. A covered third party shall notify the covered electrical corporation that is the source of the covered data within one week of the detection of a breach. Upon a breach affecting 1,000 or more customers, whether by a covered electrical corporation or by a covered third party, the covered electrical corporation shall notify the Commission's Executive Director of security breaches of covered information within two weeks of the detection of a breach or within one week of notification by a covered third party*

of such a breach. Upon request by the Commission, electrical corporations shall notify the Commission's Executive Director of security breaches of covered information."[1]

"9(c) Training. Covered entities shall provide reasonable training to all employees and contractors who use, store or process covered information."[2]

In Attachment 1, SDG&E summarizes the required breach notifications that were made during calendar year 2012 and also includes a discussion of the privacy training that SDG&E has conducted for its employees and contractors during calendar year 2012.[3]

Additionally, section 9(e) of Attachment D to D.11-07-056 states:

9(e) Reporting Requirements. On an annual basis, each electrical corporation shall disclose to the Commission as part of an annual report required by Rule 8.b, the following information:

(1) the number of authorized third parties accessing covered information,
(2) the number of non-compliances with this rule or with contractual provisions required by this rule experienced by the utility, and the number of customers affected by each non-compliance and a detailed description of each non-compliance.

SDG&E notes that with regard to provision 9(e)(2), the number of non-compliances with the Attachment D Rules or with the contractual provisions required by the Attachment D Rules will only become apparent to SDG&E if, through its daily operations, SDG&E somehow becomes aware of such non-compliances.

SDG&E believes that it is reasonable to include the remaining section 9(e) information in its annual privacy report as well and therefore this information is included in Attachment 1.

Finally, section 4(c)(6) of the Attachment D Rules states:

4.(c)(6) On an annual basis, covered entities shall report to the Commission the number of demands received for disclosure of customer data pursuant to legal process or pursuant to situations of imminent threat to life or property and the number of customers whose records were disclosed. Upon request of the Commission, covered entities shall report additional information to the Commission on such disclosures. The Commission may make such reports publicly available without identifying the affected customers, unless making such reports public is prohibited by state or federal law or by order of the Commission.

[1] From D.11-07-056, Attachment D, p. 11. SDG&E has consulted with PG&E, SCE and the CPUC's Energy Division staff to define what would constitute a reportable breach for purposes of these reports. The definition of a "Privacy Breach" is included as Attachment 3.
[2] Ibid; p.12.
[3] SDG&E notes that section 8.c. of the Attachment D Rules calls for an "Annual Report of Breaches" that includes the breach notifications required by section 8.b. of the same rules, and this information is included in Attachment 1.

SDG&E believes that it is reasonable to include the section 4.(c)(6) information in this annual privacy report as well and therefore this information is included in Attachment 1.

D.12-08-045 includes in Attachment A a nearly identical set of rules as those set forth in the Attachment D Rules, however instead of referring to "electrical corporation," D.12-08-045 refers to "gas corporations".[4] As stated above, Attachment 1 to this report also meets the D.12-08-045 annual privacy report requirements.

[4] See, for example, Attachment D to D.11-07-056, p. 1, paragraph 1. (a) as compared with Attachment A to D.12-08-045, p. A1 paragraph 1.(a).

Attachment 1

Privacy Report of SDG&E for Calendar Year (CY) 2012

Items required to be reported by Attachment D of D.11-07-056 and Attachment A of D.12-08-045:

Section 8(b) – Notification of Breaches

Number of privacy breaches affecting 1,000 or more customers reported by SDG&E during 2012.

Nothing to report.

Section 8(c) – Breaches Affecting Covered Information

Number of breaches during calendar year ("CY') 2012 affecting Covered Information (as defined in both D.11-07-056 and D.12-08-045), whether by SDG&E or by a third party to whom SDG&E provided Covered Information.

Two incidents.

Section 9(c) – Privacy Training

Summary of privacy training conducted by SDG&E during CY 2012.

SDG&E developed an online customer privacy training course, called "Safeguarding Customer Information" that consists of three components:

1. Training video (with embedded knowledge check questions)
2. Knowledge test
    - 10 questions per test randomly selected from a pool of 13 questions
    - Must pass with at least 80% correct (unlimited retries)
3. Certification
    - 3 questions
    - Must pass with 100% correct (unlimited retries)

In 2012, a total of 2,724 SDG&E employees successfully completed this training over three phases:

1. April 2012 – The first phase was assigned to approximately 1,500 CISCO users. CISCO is our main repository of customer information and was targeted first because they have

the potential to see and handle Covered Information most frequently. Therefore, this group was determined to be the highest priority group within the company.

2. September 2012 – The second phase was assigned to approximately 200 OMS/DMS users due to the launch of a new OMS/DMS system which contains customer information.
3. November 2012 – The third phase was assigned to approximately 1,000 non-union employees in 27 SDG&E organizations that were identified through a separate effort in which SDG&E is working to catalog various customer data and who were determined to have some access to Covered Information.

In addition, SDG&E offered an in-person training on the definitions of Primary and Secondary Purposes (as defined in D.11-07-056 and D.12-08-045) provided by internal subject matter experts to various groups and individuals who were determined might benefit from a more in-depth understanding. **422** employees participated in this training during CY 2012.

Section 9(e)(1) Number of Authorized Third Parties Access Covered Information

The number of authorized third parties accessing Covered Information from SDG&E during CY 2012: **210**

Section 9(e)(2) – Non-Compliances with Attachment D Rules (D.11-07-056) / Attachment A Rules (D.12-08-045)

a. The number of non-compliances with the Attachment D Rules or with contractual provisions required by the Attachment D Rules which become known to SDG&E through its daily operations during CY2012.

While there were no known non-compliances during 2012, SDG&E has concerns about the intended meaning of the requirement to add a link to its Privacy Notice in all electronic communications. While SDG&E makes every effort to include the Privacy Notice in e-mails from employees that normally communicate with customers about their information, such as contact center representatives, it is technically infeasible, not cost-effective, not a value-add, and most likely not the intention of the requirement to ensure that such a notice in every possible communication, such as social media (i.e., Twitter, Facebook, etc.), every fax, or even every e-mail sent to a customer includes a link to the Privacy Notice.

b. The number of customers affected by each non-compliance during CY 2012.

No customers were affected by non-compliances in 2012.

c. Detailed description of each non-compliance listed in (a).

Nothing to report.

Section 4(c)(6) – Data Disclosures

The number of customers whose records were disclosed (related to demands received for disclosure of customer data pursuant to legal process or pursuant to situations of imminent threat to life or property) during CY 2012:

Number of demands received for disclosure of customer data pursuant to situations of imminent threat to life or property was **four** (**4**).

Number of customers whose records were disclosed pursuant to legal process was **4,062**.

Attachment 2

Definition of a Privacy Breach

Privacy Breach: A Privacy Breach for purposes of this report is a Security Incident[5] that results in exposure or disclosure of Covered Information outside the Covered Entity to an unauthorized party.

[5] "Security Incident" as defined in United States Code, 44 USC 3552 as follows:
The term 'incident' means an occurrence that:

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."